UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,966	09/01/2000	Daniel R. Salmonsen	003551.P015	5668

7590   12/20/2005

Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 October 2005*.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18 and 20-26* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *25 and 26* is/are allowed.

6)☒ Claim(s) *1-6,8-15,17,18,20 and 22-24* is/are rejected.

7)☒ Claim(s) *7,16 and 21* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All   b)☐ Some * c)☐ None of:

　　　　1.☐ Certified copies of the priority documents have been received.

　　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   The response of 10/31/2005 was received and considered.

2.   Claims 1-18 & 20-26 are pending.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-18 & 20-26 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

5.   Claims 14-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

Regarding claim 14, the claim recites "wherein authenticating the user" (line 1), however,

the step of authenticating the user is not recited in claim 1. *Therefore, claim 1 is understood to*

have a step reading "authenticating the user".

Regarding claim 14, the claim recites "the user", however both claim 1 and claim 14

recite "a user" and it is unclear to which user the limitation "the user" (line 3) is referring.

Regarding claim 14, there is no antecedent basis for the limitation "the user

authentication data" (lines 3-4). *Therefore, the limitation "requesting user authentication" is*

understood to read "requesting user authentication data".

Regarding claim 15, the claim recites "the user" (line 3), however claims 1, 14 and 15

recite "a user" and it is unclear to which user the limitation "the user" is referring.

Regarding claim 15, the limitation "the current user authentication" (line 2) lacks

antecedent basis. *However, in light of the above assumptions, the limitation is understood to*

read "the user authentication data".

Regarding claim 15, the limitation "the user authentication" (line 2) lacks antecedent

basis. *However, in light of the above assumptions, the limitation is understood to read "the user*

authentication data".

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7.   Claims 1 & 4-6 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent

6,636,966 to Lee et al. (**Lee**).

Regarding claims 1 & 4-6, Lee discloses determining a secure medium identification/list

of handles (col. 9, lines 17-20) from a secure medium including content, sending an encrypted

one-time session key/random challenge and the disk ID to a server (col. 9, lines 17-26),

requesting user authentication (col. 9, lines 30-33) and if the user is successfully authenticated,

receiving a decrypted copy of the encrypted one-time session key/random challenge from the

server (col. 9, lines 39-52) to enable reading of the content on the secure medium.

Regarding claim 1, Lee discloses determining a secure medium identification/list of

handles (col. 9, lines 17-20) from a secure medium including content, sending an encrypted one-

time session key/session ID and the disk ID to a server (col. 9, lines 17-26), requesting user

authentication (col. 9, lines 30-33) and if the user is successfully authenticated, receiving a

decrypted copy of the encrypted one-time session key/session ID from the server (col. 9, lines

39-52) to enable reading of the content on the secure medium.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

9.   Claims 2 & 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lee**, as

applied to claim 1 above, in view of U.S. Patent 6,236,727 to Ciacelli et al. (**Ciacelli**).

Regarding claim 2, Lee lacks streaming encrypted content from the secure medium to an

application. However, Ciacelli teaches that to insure that information is protected as it moves

from a processor to the outside, the information is encrypted in the processor and decrypted by

the receiving device (col. 3, lines 29-54). Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to modify Lee to stream encrypted

content from the secure medium to an application. One of ordinary skill in the art would have

been motivated to perform such a modification to insure that the content is protected as it moves from a processor to the outside, as taught by Ciacelli (col. 3, lines 29-54).

Regarding claim 17, Lee discloses determining a reader/storage unit to read an identification/list of handles and content (col. 9, lines 17-20) from a secure medium, a session key generation logic to generate a one-time session key/random challenge (col. 9, lines 17-26), an encryption logic to send the ID/list of handles and the session key/random challenge encrypted to a server/content key server (col. 9, lines 30-33) and an authentication logic to receive authentication from the server indicating approval to read the content of the secure medium (Fig. 2B, #230), the reader to further pass the ID to the encryption logic (col. 9, lines 17-26). Lee lacks the reader to further pass the content to the encryption logic and the encryption logic further to encrypt the content prior to sending the content to an application. However, Ciacelli teaches that to insure that information is protected as it moves from a processor to the outside, the information is encrypted in the processor and decrypted by the receiving device (col. 3, lines 29-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to stream encrypted content from the secure medium to an application and hence pass the content to the encryption logic, further encrypting the content prior to sending the content to an application. One of ordinary skill in the art would have been motivated to perform such a modification to insure that the content is protected as it moves from a processor to the outside, as taught by Ciacelli (col. 3, lines 29-54).

Regarding claim 18, Lee discloses encrypting the packet with a symmetric key (col. 11, lines 37-42).

10.   Claims 3, 8-13, 20 & 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Lee** and **Ciacelli**, as applied to claims 2 & 17 above, in view of Handbook of Applied

Cryptography by Menezes et al. (**Menezes**).

        Regarding claims 3, 8-10, Lee, as modified above, lacks the application using the one-

time session key returned by the server to decrypt the encrypted content and display the

decrypted content. However, Menezes teaches that to sent a secret session key from one entity

(A) to another (B), one can use a trusted server (T) as an intermediary (p. 554, 13.12), where A

sends an encrypted session key to T, where it is decrypted, re-encrypted and returned to A who

then sends the encrypted session key to B (p. 554, 13.12). Therefore, it would have been obvious

to one having ordinary skill in the art at the time the invention was made to modify Lee, as

modified by Ciacelli, so that Lee's server further performs the functions of a KTC and as such to

send a one-time session key to the content key server/T, receive the encrypted copy of the one-

time session key from the server and deliver the session key to the application/B. One of

ordinary skill in the art would have been motivated to perform such a modification to share a

secret session key between the storage and the host, as taught by Menezes (p. 554, 13.12).

        Regarding claim 11, Lee discloses digitally encoded music/MP3 (col. 1, lines 30-32).

        Regarding claims 12-13, Lee discloses credit card information (col. 9, lines 30-32).

        Regarding claims 20 & 22-24, Lee discloses receiving a decrypting key from the server

and discloses the possibility of requesting a payment with a credit card/authentication (col. 5

lines 54-67), but lacks explicitly streaming decryption logic to receive content from the secure

device and decrypt the content using the decryption key received from the server and play the

content. However, Menezes teaches that to sent a secret session key from one entity (A) to

another (B), one can use a trusted server (T) as an intermediary (p. 554, 13.12), where A sends

an encrypted session key to T, where it is decrypted, re-encrypted and returned to A who then

sends the encrypted session key to B (p. 554, 13.12). Therefore, it would have been obvious to

one having ordinary skill in the art at the time the invention was made to modify Lee, as

modified by Ciacelli, so that Lee's server further performs the functions of a KTC and as such to

send a one-time session key to the content key server/T, receive the encrypted copy of the one-

time session key from the server and deliver the session key to the application/B and decrypt the

content based on the key received (through the host). One of ordinary skill in the art would have

been motivated to perform such a modification to share a secret session key between the storage

and the host, as taught by Menezes (p. 554, 13.12).

11.   Claims 14-15, as best understood, are rejected under 35 U.S.C. 103(a) as being

unpatentable over **Lee**, as applied to claim 1 above, in view of U.S. Patent 6,065,403 to Subbiah

et al. (**Subbiah**).

        Regarding claim 14, Lee lacks determining if the disk ID is already associated with a user

and if the disk ID is not yet associated with the user, associating the user authentication data with

the disk ID. However, Subbiah teaches that to control access to purchased software and centrally

control the number of usable copies (col. 7, lines 26-30), a user inputs software with a unique

identifier thereon, the system requests user authentication data, determines that no users are

associated with the unique identifier and associates the unique identifier with the entered user

identification data/biometric (col. 6, lines 15-54). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify Lee to determine if

the disk ID is already associated with a user and if the disk ID is not yet associated with the user, to associate the user authentication data with the disk ID. One of ordinary skill in the art would have been motivated to perform such a modification to control access to purchased software and centrally control the number of usable copies (col. 7, lines 26-30).

Regarding claim 15, Lee, as modified above, discloses determining that the current user authentication matches the user associated with the disk ID (Subbiah, col. 6, lines 55-67).

Allowable Subject Matter

12.   Claims 25-26 are allowed.

13.   Claims 7 & 16 are objected to as being dependent upon a rejected base claim, but, as best understood, would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and were amended to overcome any rejections based on 35 U.S.C. §112 ¶2.

14.   The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 7, the prior art relied upon fails to teach or suggest an application using the content decryption key and the session key returned by the server to decrypt the content received from the secure medium and playing the decrypted content, in combination with the elements of the base claim 1 and intervening claims 4-6.

Regarding claim 16, the prior art relied upon fails to teach or suggest if the user authentication does not match the user associated with the disk ID, refusing to return the session key, thereby preventing display of the content, in combination with the elements of the base claim 1 and intervening claims 14-15.

Regarding claim 21, the prior art relied upon fails to teach or suggest wherein the

decryption key includes both the session key and a content decryption key, in combination with

the elements of the base claim 17 and intervening claim 20.

Regarding claims 25-26, the prior art relied upon fails to teach or suggest a secure device

encrypting content prior to sending the content to an application, the application comprising a

user authentication interface to send user authentication received from the user to the server, an

association logic to determine if the disk ID is associated with the user and if the disk ID is not

yet associated with the user, to associate the user authentication data with the disk ID and if the

disk ID is associated with the user, determining that the current user authentication matches the

user associated with the disk ID, to authenticate the user, a key logic to receive a decryption key

from the server if the user is successfully authenticated and a streaming decryption logic to

receive encrypted content from the secure device and decrypt the encrypted content using the key

received from the server, in combination with the other elements of the claim.

Conclusion

15.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

16.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The

examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
        Commissioner for Patents
        P.O. Box 1450
        Alexandria, VA 22313-1450
Or faxed to:
        (571) 273-8300
        (for formal communications intended for entry)
Or:
        (571) 273-3841 (Examiner's fax, for informal or draft communications, please
        label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should
be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
December 12, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100